

(21) Application No: **0700525.9**

(22) Date of Filing: **14.07.2004**

(30) Priority Data:
(31) **10/892,280** (32) **14.07.2004** (33) **US**

(86) International Application Data:
PCT/US2005/024253 En 08.07.2005

(87) International Publication Data:
WO2006/019614 En 23.02.2006

(71) Applicant(s):
Intel Corporation
2200 Mission College Boulevard,
Santa Clara, California 95052,
United States of America

(72) Inventor(s):
James Sutton II
Clifford Hall
Ernest Brickell
David Grawrock

(continued on next page)

(51) INT CL:
H04L 9/08 (2006.01) **H04L 9/32** (2006.01)

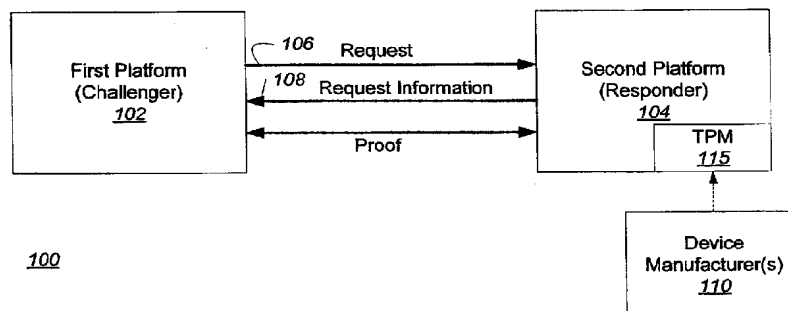
(52) UK CL (Edition X):
NOT CLASSIFIED

(56) Documents Cited by ISA:
US 6032260 A **US 20040103281 A1**
MENEZES, VANSTONE, OORSCHOT, "Handbook of
Applied Cryptography", 1997, MENEZES, VANSTONE,
OORSCHOT, USA, XP002394428.

(58) Field of Search by ISA:
INT CL **H04L**
Other: **EPO-Internal, WPI Data, PAJ, INSPEC.**

(54) Abstract Title: **Method of delivering direct proof private keys in signed groups to devices using a distribution CD**

(57) Delivering a Direct Proof private key in a signed group of keys to a device installed in a client computer system in the field may be accomplished in a secure manner without requiring significant non-volatile storage in the device. A unique pseudo-random value is generated and stored along with a group number in the device at manufacturing time. The pseudo-random value is used to generate a symmetric key for encrypting a data structure holding a Direct Proof private key and a private key digest associated with the device. The resulting encrypted data structure is stored in a signed group of keys (e.g., a signed group record) on a removable storage medium (such as a CD or DVD), and distributed to the owner of the client computer system. When the device is initialized on the client computer system, the system checks if a localized encrypted data structure is present in the system. If not, the system obtains the associated signed group record of encrypted data structures from the removable storage medium, and verifies the signed group record. The device decrypts the encrypted data structure using a symmetric key regenerated from its stored pseudo-random value to obtain the Direct Proof private key, when the group record is valid. If the private key is valid, it may be used for subsequent authentication processing by the device in the client computer system.



100

GB 2439160 A continuation

(74) Agent and/or Address for Service:
Harrison Goddard Foote
Fountain Precinct, Balm Green,
SHEFFIELD, S1 2JA, United Kingdom